CROWDSTRIKE

FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Streaming the threat detection and response lifecycle with speed, automation and unrivaled visibility

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. All endpoint activity is also streamed to the CrowdStrike Falcon® platform so that security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

FALCON ENDPOINT DETECTION AND RESPONSE (EDR)

- **Respond decisively :** Act against adversaries in real time to stop attacks before they become breaches. Powerful response actions allow you to contain and investigate compromised systems, and Falcon Real Time Response capabilities provide direct access to endpoints under investigation. This allows security responders to run actions on the system and eradicate threats with surgical precision.

GAIN FULL-SPECTRUM VISIBILITY IN REAL TIME

- **See the big picture in real time:** CrowdScore delivers a simple metric that helps an organization understand its threat level in real time. This makes it easy for security leaders to quickly understand if they are under attack and assess the severity of the threat so they can coordinate the appropriate response.
- **Capture critical details for threat hunting and forensic investigations:** Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.
- **Get answers in seconds:** The CrowdStrike Threat Graph® database stores event data and answers queries in five seconds or less, even across trillions of events.
- **Recall for up to 90 days:** Falcon Insight provides a complete record of endpoint activity over time, whether your environment consists of fewer than 100 endpoints or more than 500,000.
- **Streamline IT and security operations:** Falcon Fusion is a unified cloud-scale security orchestration, automation and response (SOAR) framework, providing customizable and easy-to-use automation to simplify enterprise security workflows.
- **Understand endpoint security posture:** Falcon Insight provides a Zero Trust Assessment (ZTA) that determines endpoint health across the organization. With real-time security posture assessment, you can easily identify and update sensor policies and OS settings that are out-of-date or increase risk. Share assessment scores with CrowdStrike Zero Trust ecosystem partners for real-time conditional access enforcement.

REALIZE IMMEDIATE TIME-TO-VALUE

- **Save time, effort and money:** Cloud-enabled Falcon Insight is delivered by the CrowdStrike Falcon platform and does not require any on-premises management infrastructure.
- **Deploy in minutes:** CrowdStrike customers can deploy the cloud-delivered Falcon agent to more than 100,000 endpoints globally in less than 24 hours.
- **Be immediately operational:** With unmatched detection and visibility from Day One, Falcon Insight hits the ground running, monitoring and recording on installation without requiring reboots, finetuning, baselining or complex configuration.
- **Experience no impact on the endpoint:** With only a lightweight agent on the endpoint, searches take place in the Threat Graph database without any performance impact on endpoints or the network.

INDUSTRY RECOGNITION

CrowdStrike is recognized as a leader in endpoint protection solutions by industry analysts, independent testing organizations and security professionals. Visit the **CrowdStrike Industry Recognition webpage** for more information.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**